UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

Plaintiff,

v.

NICHOLAS PALUMBO, NATASHA PALUMBO, ECOMMERCE NATIONAL, LLC d/b/a Tollfreedeals.com, and SIP RETAIL d/b/a sipretail.com,

Defendants.

CV 20 - 473
Civil Action No.

KORMAN, J.

MANN. M.J.

DECLARATION OF MARCY RALSTON

I, Marcy Ralston, have personal knowledge of the facts set forth below, and if called as a witness I would testify as follows:

1. I have been a Special Agent with the Social Security Administration's Office of Inspector General ("SSA OIG"), Office of Investigations since October 2004. I have been employed as a federal law enforcement officer for approximately 16 years. From approximately August 2002 until December 2003, I was employed as a Postal Inspector with the United States Postal Inspection Service. My current duties include investigating violations of Federal and State laws, primarily as they relate to misuse of social security numbers and violations of laws and regulations administered by the SSA. This includes crimes of mail fraud, identity deception, welfare fraud, theft, perjury and forgery. I have participated in multiple search warrants. I have worked several large scale, multi-agency investigations and have interviewed multiple witnesses, suspects and cooperating individuals as a part of my duties. Before this, I received a Bachelor's Degree from Indiana University in Criminal Justice in 1997. I have attended twelve weeks of

federal law enforcement training from the Inspection Service, as well as continuing education with SSA-OIG.

2. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained during my participation in this investigation, information from other individuals including other law enforcement officers, complainants, and other parties, witness interviews, and my review of documents, public records, USPIS records, and other sources. Because this declaration is submitted for the limited purpose of establishing probable cause in support of the application for a temporary restraining order, it does not set forth each and every fact that I learned during the course of this investigation.

3. SSA Imposter fraud has resulted in the filing of hundreds of thousands of complaints with the Administration in just the last fifteen months. Specifically, analysis of our complaints database reveals 465,000 complaints about fraudulent telephone impersonation of the Administration between October 1, 2018 and September 30, 2019; these complaints reflect aggregated losses of over $14 million.

4. In addition, the Federal Trade Commission ("FTC") collects complaints in its Consumer Sentinel database on SSA and other government imposter scams. For 2018, the FTC received more than 39,000 fraud complaints about SSA imposters, with related victim losses of approximately $11.5 million. SSA imposter fraud complaints for 2019 include approximately 166,000 complaints relating more than $37 million in losses.[1] In my experience, these complaint

[1] Regarding government imposter fraud more broadly and not limited just to SSA imposters, the FTC's Consumer Sentinel database contains 255,223 complaints reflecting $128,479,054 in losses for 2018, and 389,563 complaints reflecting $152,946,623 in losses for 2019.

numbers substantially underrepresent the extent of fraudulent activity because most victims do not report their losses to the government.

OVERVIEW OF DEFENDANTS' WIRE FRAUD SCHEME

5. This investigation involves a wire fraud scheme conducted and facilitated by husband and wife Nicholas and Natasha Palumbo ("the Palumbos") through the entities Ecommerce National LLC d/b/a TollFreeDeals.com ("TollFreeDeals") and SIP Retail, LLC d/b/a SIPRetail.com ("SIP Retail") (collectively, "Defendants"). The Palumbos operate and control the named entities from their home in Paradise Valley, Arizona.

6. As relevant to this Declaration, "robocalling" refers to an automated process of placing large volumes of telephone calls over the internet in order to deliver recorded messages, in contrast to calls placed one at a time by a live person. SSA OIG is investigating criminal schemes perpetrated by individuals operating one or more call centers located in India and other foreign locations. Fraudsters at the call centers impersonate government agencies and other entities – including the SSA, other government agencies, and businesses – and place millions of robocalls to phones in the United States. These robocalls convey recorded messages instructing the recipients to contact the impersonated entity regarding problems with their social security numbers, missed court dates, imminent asset freezes, and other such lies that are intended to secure the recipient into establishing phone contact with a criminal. In all of these schemes, the criminals attempt to defraud and extort money from anyone who contacts them in response to their messages.

7. Since at least 2016, despite repeated warnings from various government entities and industry actors, the Palumbos and the entities they control have provided robocallers with unfettered access to the U.S. phone system and thus the ability to deluge U.S. residents with

millions of fraudulent robocalls. The Palumbos, through their companies, have also provided fraudsters with toll-free phone numbers used in furtherance of the robocall fraud schemes that allow victims to return calls to the fraudsters in foreign locations at what appears to the potential victim to be a legitimate U.S. toll-free phone number.

8. Defendants' participation in these fraudulent robocall schemes is essential to the success of the schemes. Without someone willing to accept the fraudsters' robocall traffic into the U.S. telephone system, even though the fraudsters have internet access they would be unable to contact any potential victims in the first instance. The Palumbos provide the crucial interface between foreign internet-based phone traffic and the U.S. telephone system, and our investigation reveals that they do so with full knowledge that they are participating in massive frauds. Similarly, by providing toll-free services, Defendants not only enable initial contact with potential victims, but also provide legitimate U.S. toll-free numbers that cloak the fraud in a façade of legitimacy and allow the unwitting to become victims when they return calls to fraudsters after they receive a robocall voicemail message.

9. The robocall imposters in this investigation use a variety of methods to receive funds from victims, including but not limited to asking victims to: purchase gift cards or other stored value cards and transmit the numbers from the back of the cards to the fraudsters; send bank wires; and send cash payments by overnight carrier.

10. Victims will often send these funds to individuals referred to by law enforcement as "money mules" located in the United States, who receive and collect victim payment funds from fraud schemes, and then conduct transactions on behalf of their "handlers," who will instruct them what to do with the funds. "Money mules" will often send money from the United States back to India, via money transmitting businesses, and/or pay the business expenses for the call centers,

including paying U.S. based companies that are helping to route scam calls to U.S. victims. These payments will often consist of cash deposits into the bank accounts of the U.S. based companies.

11. In the course of this investigation, we have learned that TollFreeDeals and SIP Retail have transmitted robocalls as part of numerous fraudulent robocalling schemes, including:

a) SSA Imposters – SSA Imposters send recorded messages falsely claiming that the recipient's social security number has been used in criminal activity, the recipient's social security benefits will be suspended, the recipient failed to appear before a grand jury and faces imminent arrest, or the recipient's social security number will be terminated. When an individual calls back or connects to the fraudster, the fraudster claims to be an SSA employee and typically tells the individual to transfer substantial funds to the SSA for safekeeping until the individual is issued a new social security number, at which point the individual's funds will be returned.

b) Internal Revenue Service ("IRS") Imposters: IRS imposters send recorded messages falsely claiming that the recipient has been implicated in tax fraud, the individual has avoided attempts to enforce criminal laws, the individual has avoided court appearances, or the individual faces imminent arrest. When a recipient calls back or connects to the fraudster, the fraudster claims to be an IRS or Treasury employee and typically tells the recipient to transfer funds to the IRS to resolve various fictitious tax and legal liabilities, or for safekeeping in order to avoid seizure of assets.

c) United States Citizenship and Immigration Services ("USCIS") Imposters: USCIS imposters send recorded messages falsely claiming that the recipient has failed to fill out immigration forms correctly, the recipient faces imminent arrest or

deportation, that the recipient's home country has taken formal action against the recipient that may result in deportation, or the recipient has transferred money in a way that will result in deportation. When a recipient calls back or connects to the fraudster, the fraudster claims to be a USCIS employee and typically tells the recipient to pay various fees or fines to avoid immigration consequences.

d) Tech Support Imposters: Fraudsters operating tech support scams impersonate various well-known tech companies, such as Apple or Microsoft, and send recorded messages falsely claiming that the recipient has computer security problems that require assistance. When an individual connects with the fraudster, the fraudster often convinces the individual to pay for fictitious tech support and computer security services, and to allow the fraudster remote access to the victim's bank accounts.

e) Loan Approval Scams: Fraudsters operating loan approval scams leave messages impersonating a "lender" offering a great, guaranteed rate on a "pre-approved" loan. When a call recipient connects with the fraudster, the fraudster will emphasize that a poor credit history does not matter, and all the call recipient has to do to secure the pre-approved loan is a pay a one-time fee up front.

TECHNOLOGIES USED IN THE ROBOCALLING FRAUD SCHEMES

12. The technical ability to place the fraudulent calls at issue in the investigation is dependent on (1) voice-over-internet-protocol ("VoIP")[2] calling and related technology to create the calls, and (2) a "gateway carrier" to introduce the foreign call traffic into the U.S. phone system.

[2] VoIP stands for voice-over-internet protocol and allows users to place phone calls over a broadband internet connection.

In the telecommunications industry, the term "gateway carrier" refers to a U.S. based person or entity that agrees with a foreign person or entity (often by contract) to accept foreign-source VoIP telephone traffic. VoIP uses a broadband internet connection – as opposed to an analog traditional phone line – to place phone calls locally, long distance, and internationally, without regard to whether the call recipient uses a cellular phone or a traditional wired phone. The technology employed by modern telecommunication providers mediates between digital VoIP signals and regular telephone signals so that communication is seamless between VoIP and non-VoIP users at either end. VoIP is used in the schemes both to place robocalls to U.S. phones and to communicate with individuals who either answer the robocall or call the number contained in the recorded robocall message.

13. VoIP relies upon a set of rules for electronic communication called Session Initiation Protocol ("SIP"). Much like the way browsing websites on the Internet use HyperText Transfer Protocol ("HTTP") to initiate and conduct information exchanges between devices through exchanges of packets of information, SIP is a set of rules used to initiate and terminate live sessions for things such as voice and video communication between two or more points connected to the Internet. Both SIP voice communication and HTTP web-browsing rely on exchanging data packets between two points. For example, web browsing via HTTP requires an individual to request information from another point on the internet, usually by clicking on a hyperlink or entering a web address in a browser's address bar, usually preceded by "http://www," which tells the device that it is making a request for information on the World Wide Web via HTTP. A device receiving that request will send back information to the requesting device, and thus, the requesting device will display the requested website.

14. Similarly, a voice call via SIP starts as a data packet sent to initiate a call, a responsive packet sent back that indicates whether the call has been answered, and numerous other packets transiting back and forth; amongst these data packets is information that machines at either end turn into audible signals, i.e., a conversation that can be heard by the participants. In the case of robocalls, a recorded message is transmitted once the call is answered by a live person or by voicemail.

15. Robocalls should not be understood as traditional telephone calls, but rather, requests for information and responsive data packets transiting the internet via SIP. An outgoing robocall begins as a request for information sent by an automatic telephone dialing system known as an "autodialer" that—in conjunction with VoIP services—enables the caller to make millions of sequential requests for information (i.e., outbound VoIP phone calls) in a very short time. A VoIP autodialer is a specialized type of telecommunications equipment having the capacity to (1) store or produce telephone numbers to be called, and (2) request responsive information from devices at the other end of the call, i.e., dial the telephone numbers. The autodialer's requests for information are directed to devices (here, telephones) that send back responsive information when the call is answered either by a live person or the person's voicemail. When the autodialer receives the information from the called device indicating that the call is answered, the autodialer will then send information back to that device (the phone) in the form of a recorded message. As relevant here, fraudsters created the recorded message that conveys false threats while impersonating a U.S. agency or the other entities described above.

16. A fraudster making these robocalls can not only send a recorded message to the potential victim's phone, but can misrepresent the origin of the call on the call recipient's caller ID. Normally, a recipient's caller ID will display information identifying the caller by means of a

telephone number that is automatically displayed because the caller owns the right to use that phone number; however, many VoIP software packages allow the caller to specify the information appearing on the call recipient's caller ID, much in the same way an email's subject line can be edited to state whatever the sender wishes. This practice of specifying what appears on the recipient's caller ID is called "spoofing." This feature of VoIP technology permits a caller with an illicit motive to spoof a legitimate phone number, such as that belonging to a government entity, in order to cloak the fraudsters with indicia of authority and induce the recipients to answer the call. Spoofing also encourages potential victims to return calls when they look up the spoofed number and see that it is a number used by an official government entity. In these robocalling schemes, spoofing serves the purpose of deceiving the potential victim about who is calling them.

17. Spoofing any phone number is a simple matter of editing an SIP file to state the desired representation on the caller ID. These files can then be loaded into an autodialer to become robocalls, replicated millions of times with the spoofed, fraudulent caller ID information.

18. The fraudulent robocalls generally leave prerecorded, threatening messages for recipients. Some of the fraudulent messages direct the recipient to press a key to speak with a live operator. Other fraudulent messages leave a domestic telephone number as a "call-back" number. In either case, whether the recipient presses a key or calls the call-back number, the recipient will be connected to a fraudster in a foreign call center.

19. A gateway carrier is also essential to these fraud schemes perpetrated through these robocall schemes. Foreign call centers and VoIP carriers cannot connect VoIP phone traffic directly to the U.S. telephone system from a foreign location without the assistance of a U.S.-based telecommunications provider willing to accept the foreign call traffic. For example, a fraudulent call center in India cannot directly upload tens of millions of robocalls to the U.S. telephone

system, even where they have broadband internet and VoIP service. Foreign VoIP telephone traffic cannot enter the U.S. telephone system without travelling through a gateway carrier willing to accept the foreign traffic and introduce it to the U.S. telephone system. In the course of this investigation, SSA OIG has determined that Defendants act as gateway carriers for calls originating abroad that are bound for the United States. In the context of the schemes, fraudulent robocalls are "US terminat[ed]" calls, and return calls to fraudsters in other countries are "international voice terminat[ed]" calls.

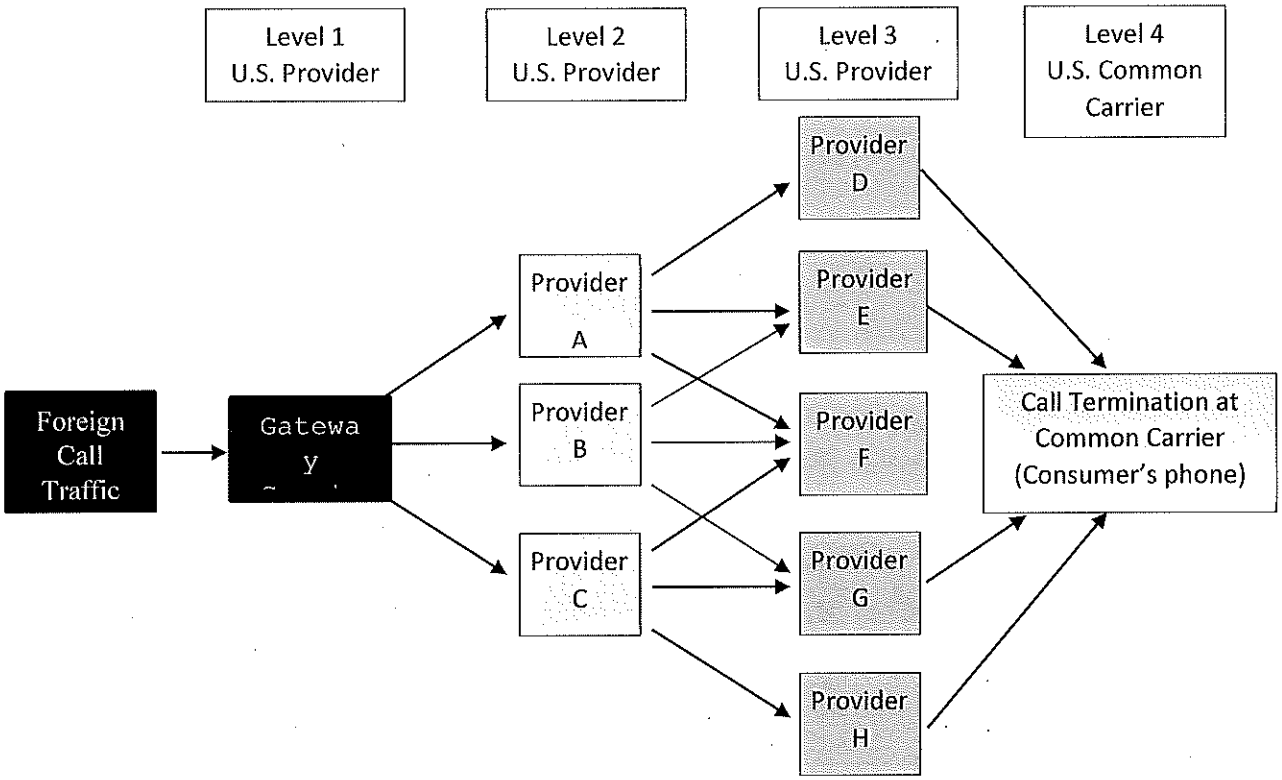
20. In the course of this investigation, I learned that with little more than off-the-shelf VoIP technology, an autodialer, and a business relationship with a gateway carrier, any individual or entity with a broadband internet connection can introduce unlimited numbers of robocalls into the U.S. telephone system from any location in the world.

LEAST-COST CALL ROUTING AND TRACEBACKS

21. When foreign call centers route fraudulent robocalls through Defendants to recipients in the United States through VoIP technology, the calls typically pass through many different VoIP carriers. First, the calls typically pass from a foreign VoIP carrier to Defendants as the U.S. gateway carrier. From Defendants, calls typically pass through multiple other carriers until they reach a common carrier such as AT&T or Verizon. Consumer-facing companies like Verizon and AT&T are known in the industry as "common carriers."

22. With modern telecommunications infrastructure, outbound VoIP calls do not take a defined path from their origin to the final destination. Rather, the system routes calls through automated equipment that determines the lowest possible connection cost at each routing step, depending on preexisting contractual relationships between the various entities. Typically, the company at each routing step will have numerous existing contracts through which it can route

outbound calls through intermediate providers to the common carriers as the last routing step before an individual in the United States can answer the call. This automated routing process is called "least-cost routing," illustrated in the following diagram beginning with a first-level U.S. gateway carrier:



In this simple example, arrows represent possible routing paths between providers based on preexisting contracts. Here, the gateway carrier has three contracts with second-level U.S. providers A, B, and C, each of which in turn has three contracts with third-level providers further into the U.S. phone system (denoted by Providers D, E, F, G, and H). Each of the third-level providers is able to pass calls to the fourth-level common carrier that provides telephone service to the U.S. individual. The call will move through one of many paths, depending on the effective contract terms between the gateway carrier, providers, and common carriers at the time the call is

routed that achieve the lowest cost to transmit the call, i.e., "least-cost routing." In real-world application, least-cost routing may involve more than four levels of U.S. companies.

23. In light of least-cost routing and the prevalence of spoofing telephone numbers, identifying the source of any specific robocall requires a labor-intensive process known in the telecommunications industry as "traceback." In order to conduct the traceback, an investigator must trace backwards each individual "hop" the call took in its least-cost-routing journey from the gateway carrier. For example and referencing the diagram above, the common carrier will be able to query its own system and determine which Level 3 Provider it received the call from, but it will not be able to see beyond that. The common carrier must contact the Level 3 Provider and ask that carrier to determine from its records what Level 2 Provider it received the call from. The common carrier must then contact the Level 2 Provider and ask them to determine which Level 1 provider they received the call from. This process continues at each "hop" until a provider identifies a foreign source – that carrier is then the "gateway carrier" that permitted the foreign telephone traffic to enter the U.S. phone system.

DEFENDANTS' ROLE IN AND KNOWLEDGE OF ROBOCALLING WIRE FRAUD CONSPIRACIES

24. Documents and other evidence obtained and reviewed in the course of this investigation, including Arizona Secretary of State and Arizona Corporation Commission records, the FCC 499 Filer Database, and a review of LinkedIn profiles, have revealed that Nicholas Palumbo has been the Chief Executive Officer of Ecommerce National LLC d/b/a TollFreeDeals.com ("TollFreeDeals") since approximately 2003. Those records further demonstrate that since at least 2016, Nicholas and Natasha Palumbo have operated TollFreeDeals

as a VoIP carrier, originally out of their home in Scottsdale, Arizona, and since mid-2019 out of their current home in Paradise Valley, Arizona.

25. As of January 25, 2020, the TollFreeDeals.com website identifies Nicholas Palumbo as the President/Founder of TollFreeDeals.com, and Natasha Palumbo as the Vice President of Business Development. Through TollFreeDeals, the Palumbos provide inbound VoIP calling to the United States (also known as "U.S. VoIP termination," because the calls "terminate" in the United States) to customers located both here in the United States and abroad. Defendants provide unrestricted VoIP dialing, meaning that they place no restriction on the number of calls their customers can place or the duration of those calls.

26. Through TollFreeDeals, the Palumbos specifically cater to call centers placing robocalls. The company's website states, "TollFreeDeals.com is your premier connection for call center and dialer termination. We are always looking for the best call center routes in the telecom industry. We specialize in short call duration traffic or call center traffic. We understand there is a need for it and we want to help you find all the channels you need!" The "FAQs" page of the website states, "Do you handle CC (Call Center)/Dialer Traffic? Yes – unlike many carriers we will handle your dialer and call center voip termination minutes." The website header also contains the statement "Call Center Minutes Terminated," followed by a number that updates every few seconds. As of January 23, 2020, that number was 10,491,500,323. Based on SSA OIG's investigation and as described above, all foreign fraudsters committing SSA impersonation fraud, as well as other government impersonation fraud and tech support impersonation fraud utilize robocalls and call centers. Defendants specifically market their U.S. call termination services to these types of customers.

27. A review of Arizona Corporation Commission records revealed that Natasha Palumbo is the registered owner and CEO of SIP Retail LLC, and has served in this capacity since registering the company on August 29, 2017. Arizona Corporation Commission records also reveal that Nicholas Palumbo is an officer/agent of SIP Retail, and that SIP Retail's current statutory agent address is the same as that for TollFreeDeals – the Palumbos' current home address in Paradise Valley, Arizona. I also viewed the website for SIP Retail, which lists Natasha Palumbo as the CEO and Founder and offers VoIP call termination services into the United States, just like TollFreeDeals. SIP Retail's website is nearly identical to the website for TollFreeDeals, including listing the same phone number for customer inquiries.

28. The websites for both TollFreeDeals and SIP Retail state that the companies use the switching platform Sip Navigator to carry VoIP termination traffic.

29. Over the past two years, Defendants received many notices, inquiries, warnings, complaints, and subpoenas concerning fraudulent robocalls transiting their systems. These warnings and inquiries came from other telecommunications companies, an industry trade group, and law enforcement agencies. Further, a review of the call detail records in the Palumbos' possession reveals that the call traffic transmitted by the majority of their customers is filled with the indicia of fraud. Nevertheless, Defendants continue to enable these massive fraud schemes to be perpetrated on U.S. individuals.

Warnings and Traceback Requests from USTelecom

30. USTelecom is a nonprofit trade association for the U.S. broadband and communications industry. USTelecom has developed an Industry Traceback Group across the telephonic communications industry to trace robocalls to their sources. Based on tracebacks

conducted with the assistance of the Industry Traceback Group, SSA OIG has identified TollFreeDeals as the number one gateway carrier of SSA imposter calls in 2019.

31. When the Industry Traceback Group conducts a traceback of a fraudulent robocall, USTelecom sends a series of email messages, starting with the common carrier whose customer received the fraudulent robocall, and getting information from each VoIP carrier in the chain about who sent the call to that VoIP carrier. These emails are referred to below as "traceback emails."

32. The Palumbos received USTelecom traceback emails about fraudulent calls that had been transmitted through TollFreeDeals and SIP Retail. Every USTelecom traceback email stated that a suspicious call has been traced back to TollFreeDeals or SIP Retail and provided the call date and time, the source number (the number that appears on the call recipient's caller ID, as well as in the gateway carrier's call records as the source of the call) and the call recipient's phone number to allow TollFreeDeals or SIP Retail to identify the specific call at issue in its call detail records. Each email also provided a link to USTelecom's web-based traceback portal, where further information is provided about the specific fraudulent call at issue, including a recording of the fraudulent voicemail message that was left on a recipient's voicemail. USTelecom traceback emails were sent to the Palumbos at nick@tollfreedeals.com or to help@sipretail.com.

33. Each traceback email from USTelecom included a short description of the type of fraudulent robocall at issue and the details of the fraudulent robocall campaign. Prior to August 2019, those descriptions were included in the traceback portal, but beginning in August 2019, those descriptions were also included in the text of the traceback email itself. An example of a traceback email sent to TollFreeDeals on August 14, 2019, is attached hereto as Exhibit 1. That email includes the following description of the fraud scheme:

> Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated voice claims suspicious activity on your social security number; press 1. Calls are from apparently random 8XX numbers or other geographic numbers. Call volume estimated at over a million per day. Because Caller-ID changes with each call, blocking the ANI is not effective.

The abbreviation "ANI "stands for "Automatic Number Identification," and for these purposes refers to the purported source number. Evidence obtained in this investigation indicates that, in response to traceback emails, Defendants blocked the single source number identified in the each email.

34. The traceback emails include a hyperlink that when clicked leads to USTelecom's online traceback portal, specifically, to a page with information regarding the specific fraudulent robocall that was the subject of the email. The portal includes audio of the voicemail message left as part of this SSA imposter robocalling campaign. I listened to the recorded audio linked to a call transmitted by TollFreeDeals on December 19, 2019, which states:

> We have been forced to suspend your social security number with immediate effect. Due to this, all your social benefits will be cancelled until further clearance. In case you feel this is due to an error, you may connect with legal [unintelligible] Social Security Administration. In order to connect with a Social Security Administration officer, press one now. In case we do not hear from you your social will be blocked permanently. To connect with the officer now, press 1 and you will automatically be connected with the concern departments. We did not receive any input. Dear citizen, in order to speak with Social Security personal regarding your social security, press 1 and this automated system will connect you with the officials. Press….

35. On June 3, 2019, USTelecom sent a traceback email to TollFreeDeals regarding an SSA imposter call. A consultant hired by USTelecom named David Frankel then corresponded directly with Nicholas Palumbo regarding the original SSA impersonation call traceback. In response, Nicholas Palumbo identified Company A, an India-based telecommunications company,

as the provider that had transmitted the SSA impersonation call to TollFreeDeals. In further email correspondence over the course of the day, David Frankel identified several different calls that were all part of the same SSA impersonation fraud campaign and all appeared on caller-ID to be coming from different source numbers. Nicholas Palumbo identified all seven calls as having been transmitted to TollFreeDeals by Customer A.

36. Three days after this email exchange, victim C.E. who was later interviewed by the Postal Inspection Service, was defrauded by an SSA imposter call. TollFreeDeals call detail records show that the SSA imposter call was transmitted from Company A to TollFreeDeals and eventually to victim C.E.'s cell phone. *See* Declaration of Samuel Bracken, Postal Inspector with the United States Postal Service, dated January 27, 2020, ¶¶ 10-12.

37. Based on the volume of traceback emails that TollFreeDeals and SIP Retail have received from USTelecom, Defendants were warned repeatedly that many of their customers were transmitting millions of fraudulent robocalls. From May 2019 through January 2020, TollFreeDeals received a total of 144 notifications from USTelecom that a fraudulent robocall had been traced back to TollFreeDeals. Of these notifications, 83 referenced SSA imposter fraud calls, 24 referenced Tech Support imposter fraud calls, ten referenced IRS imposter fraud calls, and one referenced a USCIS impersonation fraud call. TollFreeDeals reported to USTelecom that it had received these 144 calls from 14 different customers, and that all of the SSA Impersonation calls traced back to the same two Indian entities.

38. From August 2019 through December 2019, USTelecom notified SIP Retail of 35 tracebacks of fraudulent robocalls, including 19 tracebacks of SSA impersonation fraud calls, six tracebacks of Tech Support fraud calls, and one traceback of USCIS impersonation fraud calls. SIP Retail reported back to USTelecom that it had received these 35 fraudulent calls from seven

different companies, and that all 19 of the SSA impersonation calls were sent to SIP Retail by two India-based companies that sent SSA imposter calls through TollFreeDeals.

Notifications of Fraudulent Robocall Traffic From AT&T

39. In May 2017, AT&T notified Nicholas Palumbo that it had traced back to TollFreeDeals robocalls received by AT&T customers in which the source number was spoofed to show a number belonging to USCIS; another number was spoofed to show the Office of the Inspector General of the U.S. Department of Homeland Security ("DHS-OIG"). AT&T informed Nicholas Palumbo that the callers who spoke to AT&T's customers impersonated U.S. Immigration Officers, and that AT&T had confirmed with USCIS and DHS-OIG that those agencies did not make outbound calls from either of the spoofed phone numbers. Nicholas Palumbo responded that the calls had been transmitted to TollFreeDeals from an India-based customer, and that he had blocked those two specific phone numbers. Blocking specific numbers is an ineffective means to stop fraudsters who are willing and have the ability to spoof any number for their fraud calls.

40. In February 2019, AT&T notified Nicholas Palumbo that it had traced back 19 separate calls to AT&T customers that spoofed a USCIS phone number in order to "extort money from our customers." In Nicholas Palumbo's response to AT&T, he acknowledged that those calls had been transmitted to TollFreeDeals from the same India-based VoIP carrier that had transmitted the spoofed USCIS calls in 2017. Despite repeated warnings from AT&T that this customer was transmitting fraudulent government-impersonation robocalls, the Palumbos continued transmitting VoIP calls on behalf of this customer through at least as recently as June 2019.

Records of the Calls Transmitted by TollFreeDeals are Filled with Evidence of Fraud

41. SSA obtained call detail records from TollFreeDeals for all call traffic transmitted from India-based VoIP carrier Company A to TollFreeDeals between May 6, 2019 and June 30, 2019. During that period, Company A transmitted 182,023,773 calls to phones of U.S. call recipients through TollFreeDeals. These calls came from more than ten million unique source numbers, the vast majority of which were U.S. phone numbers. Based on my training and experience, there is no legitimate business purpose for which one or several foreign call centers would use millions of different U.S. source numbers to transmit calls originating abroad. This massive volume of different source numbers, as well as the ratio of source numbers to calls, is indicative of the use of random, spoofed source numbers in order to: (1) make it appear to potential victims that the calls originate in the United States, and (2) mask from legitimate U.S. carriers and law enforcement the fact that all of these millions of fraudulent calls are originating from the same source.

42. Of these more than 182 million calls, more than 2.8 million were made to phone numbers with area codes locating them within the Eastern District of New York.

43. In the call detail records related to Company A, one thousand different unique source numbers accounted for more than 90% of the calls, more than 164 million calls. SSA OIG requested records regarding these 1,000 source numbers from YouMail, a company that provides robocall-blocking software that can be downloaded for free on any cellular phone, and which maintains detailed analytics records regarding all calls blocked on behalf of its more than 10 million subscribers. Specifically, YouMail maintains data regarding the type of scam voicemails left for its customers. Records obtained from YouMail demonstrate that 79% of the top 1,000 source numbers from the Company A call detail records have been identified as sending scam

calls. Aggregating the number of calls made by each of the source numbers identified by YouMail as sending fraudulent robocalls, Company A transmitted more than 143 million fraudulent robocalls to U.S. call recipients through TollFreeDeals between May 6, 2019 and June 30, 2019. Based on YouMail's categorization of those scam calls, almost 20% (more than 31 million calls) were SSA imposter calls, another 35% (more than 57 million calls) were loan approval scams, and 14% (more than 23 million calls) were Microsoft Refund Scams,[3] a subset of Tech Support impersonation scams.

44. The Consumer Sentinel database maintained by the FTC contained consumer complaints regarding 923 of the 1,000 source numbers from the call detail records related to Company A. As of August 2019, the Consumer Sentinel database contained 58,225 complaints regarding those 923 source phone numbers.

45. SSA OIG also obtained call detail records from TollFreeDeals regarding all VoIP call traffic terminated in the United States by TollFreeDeals on behalf of all customers between May 20, 2019 and June 11, 2019. During that 23 day time period, TollFreeDeals transmitted a total of 720,008,294 calls from its customers to U.S. call recipients. TollFreeDeals also provided records to SSA-OIG demonstrating that these roughly 720 million calls were terminated on behalf of 67 unique customers. Those calls originated from more than 133 million unique source numbers, the vast majority of which were U.S. phone numbers. Of those more than 720 million calls, more than 425 million, or 59% of the total calls, lasted less than one second in duration. SSA

[3] In a Microsoft Refund Scam, call recipients receive a message stating that a tech support company is going out of business and the recipient is entitled to a refund for services previously purchased. Once a call recipient returns the call, a fraudster in a call center convinces the recipient that the tech company's refund department inadvertently refunded the call recipient thousands of dollars, rather than hundreds of dollars. The fraudster then convinces the call recipient to wire money to return the purported refund overpayment.

OIG has learned from discussions with U.S. telecommunications carriers and with employees of USTelecom, that in the telecommunications industry, such high volumes of short-duration and unanswered calls are indicative of robocalls that are unwanted by the recipients, often because they are fraudulent. Calls from Company A accounted for roughly 11% of TollFreeDeals' total call traffic during this 23 day period.

46. Of the more than 720 million calls transmitted by TollFreeDeals during this 23 day period, 24,371,682 were made to phone numbers with area codes locating them within the Eastern District of New York. More than 14 million calls had a duration of less than one second, and more than 22 million calls had a duration of less than 30 seconds.

47. Department of Justice analysts identified the top 1,000 source numbers that sent the highest volume of calls across all TollFreeDeals customers during this 23-day period. Those top 1,000 source numbers combined sent more than 169 million calls, roughly 23.5% of all calls. SSA OIG obtained records related to these 1,000 phone numbers from YouMail and from FTC's Consumer Sentinel database. FTC received complaints regarding 460 of the top 1,000 source numbers, accounting for more than 112 million calls. YouMail records revealed that 441 of the source numbers, accounting for more than 90 million were categorized as scam calls. Based on just these top 1,000 source numbers sending the highest volume of calls, 29 unique TollFreeDeals customers transmitted call traffic from source numbers that YouMail and/or FTC records associated with fraudulent robocalls.

Defendants Provide Toll Free Numbers to Foreign Robocall Fraudsters

48. Not only do Defendants knowingly pass fraudulent robocalls by the millions into the U.S. telephone system, but they also provide return-calling services to fraudsters so that potential victims can call them back. These toll-free telephone numbers and related services are

provided in the robocall message as call-back numbers, and appear to be U.S. telephone numbers and thus enable fraudsters to further deceive individuals about the robocall's origin and the identities and locations of the fraudsters at the other end of the call. In reality, what appears to the individual to be a U.S. telephone number is just a telephone number that Defendants register to an internet address designated by the fraudsters. Thus, the toll-free numbers can be used to ring telephones anywhere in the world.

49. While toll-free numbers used for return-calling purposes cannot be "spoofed" like outgoing robocalls, the use of a U.S. toll-free number in Defendants' robocalls schemes serves much the same purpose as spoofing—deception. The toll-free services provided by Defendants use VoIP technology to direct potential victims' return calls from the United States to the foreign fraudsters' call centers. The Defendants have knowingly provided toll-free numbers and associated calling services to foreign robocall fraudsters.

50. All toll-free numbers in the United States are administered by Somos, Inc., a company designated by the Federal Communications Commission ("FCC") as the national administrator of the U.S. toll-free calling system and its database. Among other functions within the industry, Somos registers "Responsible Organizations," that are authorized to provide toll-free numbers to their customers and to register those numbers in the national registry that the industry uses to direct toll-free telephone traffic. Defendants obtain toll-free numbers on behalf of their customers from one or more responsible organizations.

51. On July 31, 2019, an employee of a Responsible Organization sent the message below to Nicholas Palumbo via his @tollfreedeals.com email address:

Hello,

We received a call yesterday (at 6 pm) that we didn't answer.

> Calling Number: +844[XXXXXXX]
> Requesting to call back: 844-[XXX]-[XXXX]
>
> Please see the attached audio and screenshot of the voicemail transcript. Shut down this user immediately as it was associated with the customer account of [TollFreeDeals customer]. These types of scam calls are prohibited from our network and further fraudulent calls from the same customer account will result in termination of said customer account. The number of 844-[XXX]-[XXXX] has been removed from your account in order to protect the integrity of our network.

I listened to the audio file, and the statement below is a true and correct transcription of the audio I heard:

> tomorrow $399.99 is going to be deducted from your account for the remainder of your computer services. If you want to cancel the subscription, please press 1 to talk to our cancellation officer. Or you can call us back on our help line number 1-844-[XXX]-[XXXX]. I'll repeat the help line number 1-844-[XXX]-[XXXX]. Thank you."

52. From August 1, 2019, through August 9, 2019, the Responsible Organization sent an additional six emails to Nicholas Palumbo, notifying him that the Responsible Organization was removing eight additional toll-free numbers from the accounts of two TollFreeDeals customers, because those numbers had been shown to be used in Tech Support impersonation scams and scams impersonating Amazon customer service. In response to each email, Nicholas Palumbo responded to the effect that he had informed his customer.

53. On August 12, 2019, an employee of the Responsible Organization emailed Nicholas Palumbo and stated:

> Good afternoon Nick,
>
> I wanted to reach out to inform you that we have disabled the account of [TollFreeDeals customer] due to fraudulent complaints. Unfortunately, we do get a lot of complaints about customers under your reseller account. Our first line of defense when issues like arise we deactivate the customer's account. I am informing you that if we do receive any additional complaints about any of your other customers under your re-seller account, we will be forced to deactivate your account.

54. That same date, Nicholas Palumbo responded "I let him know," then responded further, "I will be porting clients over[.] Can't take that chance." In the telecommunications industry, to "port a number" means to move an existing phone number from one provider to another. In effect, Nicholas Palumbo was stating that he planned to take the toll-free numbers registered to his customers through the Responsible Organization who had warned him about fraudulent calls, and move those same numbers to another provider on behalf of his customers. The August 12, 2019, email correspondence referenced in this paragraph is attached as Exhibit 2.

55. On May 11, 2019, Nicholas Palumbo emailed himself a reminder to "Order 10 toll frees" for India-based VoIP carrier Company A.

Pursuant to 28 U.S.C. § 1746, I hereby declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief. Executed on January 27th, 2020, in Scottsdale, Arizona.

Marcy Ralston
Special Agent, SSA OIG

EXHIBIT 1

2019-08-14 18:16:02 UTC: Sent Formal email to nick@tollfreedeals.com

USTELECOM | THE BROADBAND ASSOCIATION

To Whom It May Concern:

By way of introduction, my name is Farhan Chughtai, and I coordinate the efforts of USTelecom's Industry Traceback Group. We are writing to request your assistance on industry efforts focused on our shared interests of protecting consumers from fraudulent, abusive or potentially unlawful robocalls. My contact information is listed below, and I would be more than happy to discuss this request with you over the phone.

A member of USTelecom's Industry Traceback Group recently received traffic from your network that has been deemed suspicious, and we are seeking your assistance in order to identify its origin (call details with date(s) are listed below). We request that you assist industry stakeholders who are engaging in traceback efforts in order to help identify the source of this potentially fraudulent, abusive or unlawful network traffic. To assist us in our efforts, **we are asking that you respond to this traceback inquiry as soon as possible, but no later than three business days from now.**

Please note that the FCC's Enforcement Bureau recently reached out to carriers that were not supporting these traceback efforts (discussed below). In addition, USTelecom has recently initiated an automated system for conducting tracebacks. We are asking that you submit your response to this inquiry via our secure on-line portal, where you can see additional detail about all traceback requests involving your network. With respect to the call details below, can you please provide us with the following:

1. Please investigate the source of this traffic and respond with the identity of the upstream carrier(s) that sent the traffic into your network, or if one of your end users originated the traffic, please state as such and identify that end user. **We ask that you use the link below to access the portal and use the drop-down selector to provide this information.**

2. If, in investigating this traffic, the end user(s) originating the traffic are able to demonstrate to you that the traffic complies with applicable United States laws and regulations, please respond via email to me with the description of the traffic, the identity of the customer, and the customer's explanation.

3. As you investigate this matter, please take appropriate action on your network to ensure compliance with applicable United States laws and regulations, and inform me of the action you have taken.

Regarding this request, USTelecom has a group of members and non-members dedicated to tracing back fraudulent, abusive, and/or unlawful traffic to its source (called the "Trusted Carrier Framework") so that such calls never reach consumers. USTelecom is a 501(c)(3) industry trade association that is coordinating the efforts of the Trusted Carrier Framework. This cooperative framework includes a broad range of industry participants (including ILECs, CLECs, VoIP providers, long distance companies, and wholesale providers), who are working to reduce the number of robocalls consumers receive and help identify their origins. This traceback framework – and others like it – operate under the auspices of the Communications Act which permit telecommunications carriers to disclose and/or permit access to Customer Proprietary Network Information (CPNI).

We invite you to join our industry traceback efforts; there is no cost to do so. Please call or email to have your preferred contact information added to our systems.

Section 222(d)(2) of the Communications Act permits telecommunications carriers to share such information in order to "protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services." Recently the FCC's Enforcement Bureau sent a series of letters – some under its Section 403 investigation authority – to carriers that have been non-responsive to USTelecom's traceback request (see here: https://docs.fcc.gov/public/attachments/DOC-354942A2.pdf). The letters "urged" carriers to "to cooperate with the USTelecom Industry Traceback Group's program aimed at identifying the source of illegal robocalls and harmful spoofed calls."

In addition, Section 2702(c)(3) of the Electronic Communications Privacy Act (ECPA) permits providers to divulge a record or other information pertaining to a subscriber to or customer of a service, "as may be necessarily incident to . . . the protection of the rights or property of the provider of that service." Given the negative impact of these calls on the rights and property of the members of USTelecom's Trusted Carrier Framework, disclosure of this information fits within that exception. To the extent that our industry effort identifies the originator of these suspicious robocalls, we first ask that mitigation efforts be taken at that source. For illegal traffic that goes unmitigated, USTelecom advises the appropriate law enforcement agencies so that they can take appropriate action against the caller, should they elect to do so. Similarly, if this industry effort fails to trace these calls their origin, USTelecom may inform the appropriate agencies about the suspicious robocalls and the point in the call path where the investigation ends.

Please feel free to consult with your counsel on this request, and do not hesitate to contact me should you have any questions, or would like to discuss.

Thanks,
Farhan

Farhan Chughtai
Director, Policy & Advocacy
USTelecom – The Broadband Association
601 New Jersey Avenue NW, Suite 600
Washington, DC 20001

Submit your response via our secure on-line portal:
https://traceback.ustelecom.org/Form/Login/r;REDACTED?t=kF9qfzR7iyG
(URL is a private login; do not share.)

Call Details for Incident #690 (new)

Date/Time:	2019-08-05 15:07:00 UTC
To:	+13013437570
From:	+18004038700
Campaign:	SSA-BenefitsCanceled
	Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated message threatens that social security benefits will be canceled. Caller-ID appears to be a random toll-free number. Called party is asked to press 1 to speak to an agent. Caller-ID is random (different on each call) so blocking the ANI is not effective.

Call Details for Incident #724 (new)

Date/Time:	2019-08-12 14:03:00 UTC
To:	+15864892755
From:	+18883716781
Campaign:	SSA-Jun2019
	Captured recordings suggest these calls are perpetrating a SERIOUS FRAUD. Caller is impersonating a federal official. Automated voice claims suspicious activity on your social security number; press 1. Calls are from apparently random 8XX numbers or other geographic numbers. Call volume estimated at over a million per day. Because Caller-ID changes with each call, blocking the ANI is not effective.

Call Details for Incident #723 (new)

Date/Time:	2019-08-12 14:10:00 UTC
To:	+12488083416
From:	+19562547097
Campaign:	SSA-Jun2019
	(see description above)

Call Details for Incident #722 (new)

Date/Time:	2019-08-12 14:40:00 UTC
To:	+12485055710
From:	+19567226365
Campaign:	SSA-Jun2019
	(see description above)

Call Details for Incident #687 (9d3h ago)

Date/Time:	2019-08-05 14:10:00 UTC
To:	+12155344889
From:	+18786525758
Campaign:	SSA-Jun2019
	(see description above)

EXHIBIT 2

On Mon, Aug 12, 2019 at 2:23 PM -0700, "JR Voltaggio" <jr@teli.net> wrote:

> Good afternoon Nick,
> I wanted to reach out to inform you that we have disabled the account of [redacted] due to fraudulent complaints. Unfortunately, we do get a lot of complaints about customers under your re-seller account. Our first line of defense when issues like arise we deactivate the customer's account. I am informing you that if we do receive any additional complaints about any of your other customers under your re-seller account, we will be forced to deactivate your account.
>
> **JR Voltaggio**
>
> teli
>
> Customer Success Manager
> Office (844) 411-1111
> jr@teli.net
> www.teli.net

To	JR Voltaggio <jr@teli.net>
From	nick palumbo <nick@tollfreedeals.com>
Date/Time - UTC+00:00 (M/d/yyyy)	8/12/2019 9:36:58 PM
Subject	Re: Account [redacted]
Body	I let him know

To	JR Voltaggio <jr@teli.net>
From	nick palumbo <nick@tollfreedeals.com>
Date/Time - UTC+00:00 (M/d/yyyy)	8/12/2019 9:37:15 PM
Subject	Re: Account [redacted]
Body	I will be porting clients over Can't take that chance